IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA v. PATRICK ALLEN WOMBLE, Defendant.	Case No. 1:22-MJ-337

AFFIDAVIT IN SUPPORT OF A
CRIMINAL COMPLAINT AND ARREST WARRANT

I, Corey S. Carnahan, Special Agent, being first duly sworn, hereby affirm and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI"), and I have been so employed since April 2022. I am currently assigned to a white-collar crime squad at the FBI's Washington Field Office. During my employment with the FBI, I have conducted and/or assisted in criminal investigations involving fraud against financial institutions, private businesses, and individuals, including investigations involving wire fraud, conspiracy, money laundering, and other related violations of Title 18 of the United States Code. I have training and experience in the enforcement of the laws of the United States, including the preparation and presentation of affidavits in support of criminal complaints.

2. The facts and information contained in this affidavit are based on my personal knowledge as well as observations of other law enforcement officials involved in this investigation. All observations that were not personally made by me were related to me by the persons who made them or by representatives of those persons. This affidavit is intended to show

only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

3. I make this affidavit in support of an application for issuance of a criminal complaint and arrest warrant for PATRICK ALLEN WOMBLE ("WOMBLE") when, in the Eastern District of Virginia, from on or about September, 2020 to on or about April 15, 2021, he knowingly transferred the proceeds of an unlawful activity with the intent to promote such unlawful activity in order to conceal the proceeds of the unlawful activity in violation of Title 18 United States Code, Section 1956(a)(1)(B) (laundering of monetary instruments).

PATRICK ALLEN WOMBLE AND RELATED ENTITIES

4. WOMBLE is a United States citizen who resides in the Northern Virginia area.

5. EOE Construction LLC is a Virginia Limited Liability Company formed on November 12, 2020. According to the Virginia State Corporation Commission, EOE Construction LLC has a purported principal place of business in Reston, Virginia. The Virginia State Corporation Commission lists the registered agent as WOMBLE with an address in Reston, Virginia, within the Eastern District of Virginia.

6. PNC, Citibank, Wells Fargo, and BB&T are financial institutions within the meaning of Title 18, United States Code, Section 20, each of which operates in the Eastern District of Virginia. The deposits of these banks are insured by the Federal Deposit Insurance Corporation.

7. Cashapp is a mobile payment service available in the United States and the United Kingdom that allows users to transfer money to one another (for a 1.5% fee for immediate transfer) using a mobile phone application.

WOMBLE'S IDENTIFIED ROLE IN THE SCHEMES TO DEFRAUD

8. According to an interview with WOMBLE, supporting records, and victim interviews, beginning at least in September 2020, and continuing through at least April 2021, WOMBLE opened multiple bank accounts at the direction of an unidentified subject ("UNSUB") whom he met on the internet.[1] WOMBLE provided his bank account information to the UNSUB for the purpose of receiving and transferring money. WOMBLE received the proceeds of at least eight Business Email Compromise ("BEC") schemes into his bank accounts and transferred the money at the direction of the UNSUB, resulting in an approximate attempted loss of over $1,300,000 and an actual loss of hundreds of thousands of dollars. As described in more detail below, WOMBLE knew the money he was receiving was the proceeds of fraud. However, WOMBLE agreed to receive and launder the fraud proceeds on behalf of the UNSUB in exchange for payment.

GENERAL DESCRIPTION OF FRAUD SCHEME

9. In a BEC, perpetrators "hack" or gain access to the e-mail accounts of a company or individual, or they create an email account that appears to the victim as if it is a legitimate business account. Once the subject has established access to the e-mail or has created a bogus email account, the perpetrator begins communicating directly with the victim using the compromised or "spoofed" e-mail address. Often, only an examination of the full e-mail header data allows for the identification of the actual e-mail address.

10. When the timing is right, often when a real transaction is due for payment, the scammers send a bogus email to a targeted employee in the finance office—often a bookkeeper, accountant, controller, or chief financial officer. Often these emails may include correct invoices

[1] All dates and amounts throughout this Affidavit are approximate.

or other documentation and may come directly after a trusted vendor has requested payment and include the trusted vendor's correspondence in the email. The bogus email may advise the targeted employee that the banking information for the trusted vendor has changed. The employee of the victim company will then make a payment via wire transfer to bank accounts controlled by the perpetrator. Soon after the wire transfer is completed, the fraud proceeds are withdrawn from the bank account and the funds are laundered.

11. In order to launder the funds, perpetrators will often rely on other individuals to receive funds and transfer them into different bank accounts and/or into cash. These transactions obscure the source and destination of the funds, making it harder to identify the perpetrator of the fraud. Additionally, these bank accounts may also be used for legitimate transactions, further obscuring the source and destination of the criminally derived money. The individuals will typically receive a percentage of the funds transferred as a payment. Based on my training and experience, I know that these transactions will often occur immediately or very shortly after funds are initially deposited in an account to minimize the time that a bank or a victim might have to recognize the fraud and retrieve their money. Launderers typically use several methods to rapidly deplete account funds. Methods include purchases of cashier's checks, high dollar amount cash withdrawals, rapid and successive ATM withdrawals, and multiple transfers through mobile payment services such as Cashapp. Cash withdrawals are often used to buy virtual currency.

12. As described in more detail below, WOMBLE used bank accounts at PNC, Citibank, Wells Fargo, and BB&T to receive fraudulent wire transfers from businesses victimized by a BEC and launder those funds.

BANK ACCOUNTS INVOLVED IN THE SCHEME

13. According to bank records, on November 17, 2017, WOMBLE opened a personal checking account ending in 8562 at Wells Fargo ("Wells Fargo 8562"). Wells Fargo bank statements show that WOMBLE used the account for personal expenses and to receive military retirement benefits. WOMBLE also used Wells Fargo 8562 to receive the proceeds of multiple BECs.

14. On November 19, 2020, WOMBLE went to a PNC branch and opened a PNC bank business checking account ending in 4399 ("PNC 4399") in the name of EOE Construction LLC. The account application lists the signatory as WOMBLE. December 2020 and January 2021 statements show that WOMBLE received only three legitimate deposits during this time: a $2,100 cash deposit on December 2, 2020, a check from Wells Fargo Bank for $11.87 on December 12, 2020, and a military retirement payment for $1,071.50 on December 31, 2020. As discussed below, all other deposits during this time period were identified as fraudulent.

15. On January 22, 2021, WOMBLE went to a BB&T branch and opened a business checking account ending in 8217 ("BB&T 8217") in the name of EOE construction LLC. The account application lists the signatory as WOMBLE. Bank statements show BB&T 8217 received two deposits—a $100 initial deposit and an identified fraudulent $180,000 deposit discussed below—before being closed in February of 2021.

16. On March 15, 2021, WOMBLE went to a Citibank branch and opened a business checking account ending in 0831 ("Citi 0831") in the name of EOE Construction LLC. The account application lists the signatory as WOMBLE. Bank statements show one $50 deposit in March 2021 and two identified fraudulent deposits in April 2021 that are discussed below. All other transactions are cash withdrawals.

PROBABLE CAUSE

A. Bank Account 1: Wells Fargo 8562

Victim-1

17. Victim-1 is a construction company located in Zolfo Springs, Florida. According to an interview with the owner of the company and his mother, on September 23, 2020, an administrator for Victim-1 received an invoice via email from someone purporting to represent a business associate requesting a wire payment of $12,977 be sent to Wells Fargo 8562. The administrator was expecting the invoice; however, they usually paid the associate by check. According to bank records, on September 24, 2020, Victim-1's employee complied with the instructions and wired $12,977 to Wells Fargo 8562.

18. Bank records show that on September 24, 2020, WOMBLE received the wire from Victim-1 of $12,977 into his Wells Fargo checking account ending in 8562. From September 24, 2020, to September 25, 2020, WOMBLE withdrew $5,050 in cash over five transactions from Wells Fargo 8562 out of ATMs at 2264 Hunters Woods Plaza, Reston, VA; 2500 Caton Hill Road, Woodbridge, VA; 2575 John Milton Drive, Herndon, VA; and inside a Wells Fargo location. All four locations are in the Eastern District of Virginia. On September 25, 2020, and September 28, 2020, WOMBLE sent $6,803 from Wells Fargo 8562 to his Cashapp account.

19. According to the interview with Victim-1's owner and his mother, Victim-1's administrator learned of the fraud when the real business associate inquired about the status of the payment. It was then discovered by the administrator that the associate's email had been compromised. Victim-1 did not know Womble or give him permission to take the funds, nor did Womble perform any work for Victim-1.

20. Based on my training and experience, these Wells Fargo 8562 account transactions are not typical of legitimate business activity. Specifically, launderers typically use several methods to rapidly deplete account funds. Methods include, rapid and successive ATM withdrawals, and multiple transfers through mobile payment services such as Cashapp. Additionally, the fact that WOMBLE did not transfer the full value of the $12,977 out of his account is consistent with him keeping a portion of the proceeds for himself, as would be expected in a BEC money laundering operation.

Victim-2

21. Victim-2 is a construction company located in Purcellville, Virginia, which is within the Eastern District of Virginia. According to an interview with the Controller for Victim-2, on October 27, 2020, an employee of the company received an email purporting to be from a vendor that Victim-2 regularly uses. The email came from an address that appeared to be identical to the real vendor's email address. The email provided new banking instructions for ACH and wire transactions. The instructions advised Victim-2 to make payment to Wells Fargo 8562 in the name of the vendor. Bank records show that on October 29, 2020, two ACH transfers were sent from Victim-2's M&T account to WOMBLE's Wells Fargo 8562 totaling $535,412.25. The same day, WOMBLE transferred $40,000 of the money to his separate Wells Fargo Savings account #XXXXXX8018, a bank account located in the Eastern District of Virginia.

22. That same day, Victim-2's Controller stated that the company realized the transactions were fraudulent when they contacted the real vendor in a new email thread. Victim-2 immediately notified M&T Bank of the transactions. M&T notified Wells Fargo that the payments were sent due to a BEC of Victim-2. WOMBLE transferred the $40,000 from the

separate Wells Fargo savings account back to Wells Fargo 8562 that same day. On October 30, 2020 the full $535,412.25 was returned to Victim-2.

23. Based on my training and experience, these Wells Fargo 8562 account transactions are not typical of legitimate business activity. Specifically, the size of these transactions and the short timeframe between incoming and outgoing wires/withdrawals suggest fraudulent activity.

Victim-3

24. Victim-3 is a development company located in Palm Springs, Florida. In an interview, the Assistant Controller and the Controller of the company reported that on October 28, 2021 and November 10, 2020, they received an email that appeared to come from a business associate containing invoices and wire transfer instructions. Victim-3 worked with this business associate and expected the invoices they sent. The instructions requested $30,413.40 be sent to Wells Fargo 8562. The email address was similar to the legitimate business associate company email with only minor changes in the letters. According to bank records, on November 10, 2020, WOMBLE received the $30,413.40 from Victim-3 into his Wells Fargo 8562 account. On November 12, 2020, WOMBLE withdrew the money in two cashier's checks for amounts of $14,200 and $10,700 and sent $4,000 from Wells Fargo 8562 to his Cashapp account. WOMBLE also made two cash withdrawals from Wells Fargo 8562 out of the Wells Fargo ATM at 2575 John Milton Dr, Herndon, VA, within the Eastern District of Virginia, on November 10th and 11th.

25. The Assistant Controller and the Controller of Victim-3 stated that the company did not realize the wire was fraudulent until several days after the transaction when the legitimate business associate contacted Victim-3 about the money. Victim-3 notified their bank but were

unable to recover any of the lost amount. Victim-3 did not know Womble, nor did Victim-3 give Womble permission to take the money. Womble did not perform any services for Victim-3.

26. Based on my training and experience, the Wells Fargo 8562 account transactions are not typical of legitimate business activity. Specifically, launderers typically use several methods to rapidly deplete account funds as occurred here. Methods include purchases of cashier's checks, rapid and successive ATM withdrawals, and multiple transfers through mobile payment services such as Cashapp.

B. Bank Account 2: PNC 4399

Victim-4

27. Victim-4 is an architecture firm located in Charleston, South Carolina. Bank records show that on December 24, 2020, WOMBLE received an ACH transaction from Victim-4 for $206,011.20 into PNC 4399.[2] WOMBLE withdrew $800 from PNC 4399 out of an ATM that same day at 2551 John Milton Drive, Herndon Virginia. On December 26, 2020, WOMBLE purchased a cashier's check from PNC 4399 for $750 written with a memo line "business." On December 28, 2020, through January 15, 2021, WOMBLE sent $7,500 from PNC 4399 to his Cashapp account over five transactions and withdrew $193,310.50 from the account in cash from the PNC Bank located at 2551 John Milton Drive, Herndon Virginia over seven transactions. During this period, bank records show that WOMBLE used money in this account to pay bills, eat out at restaurants, and make purchases at various stores in the Northern Virginia area.

28. According to an FBI Internet Crime Complaint Center ("IC3") report, Victim-4 stated that on March 4, 2021 a partner's email was compromised and the $206,011.20 ACH was

[2] As stated above, bank records show WOMBLE received only three legitimate deposits for the duration of PNC 4399 being open.

fraudulent and the result of the BEC. Victim-4 did not know Womble, nor give him permission to take the funds. Womble did not perform any work for Victim-4.

29. Based on my training and experience, the PNC 4399 account transactions are not typical of legitimate business activity. Launderers typically use several methods to rapidly deplete account funds. Methods include purchases of cashier's checks, high dollar amount cash withdrawals, rapid and successive ATM withdrawals, and multiple transfers through mobile payment services such as Cashapp. Specifically, in this case, WOMBLE took high dollar amounts out of his account through ATMs, cashier's check, and Cashapp within four days of receiving a large wire transaction. Additionally, the fact that WOMBLE did not transfer the full value of the $206,011.20 out of his account and spent approximately $2,200 over the course of 26 days after the fraudulent deposit on personal expenses is consistent with him keeping a portion of the proceeds for himself, as would be expected in a BEC money laundering operation.

Victim-5

30. Victim-5 is an individual living in Greybull, Wyoming. Bank records show that on January 19, 2021, WOMBLE received a wire transfer from Victim-5 of $108,000 into PNC 4399. Bank records show that on January 21, 2021, and January 22, 2021, WOMBLE sent $7,460 to his CashApp account from PNC 4399. On January 21, 2021, bank records show that WOMBLE visited the PNC Bank located at 2551 John Milton Dr. Herndon, Va. 20171, within the Eastern District of Virginia, purchased two cashier's checks in amounts of $35,850.90 and $57,450.50 from PNC 4399, and deposited them into bank accounts in the name of Rome Associated Group Inc.

31. According to an FBI IC3 report, on January 20, 2021, PNC received a wire recall request from Victim-5's bank stating that Victim-5's email was hacked and Victim-5 had received

fraudulent wire instructions. Victim-5's bank reported the incident to the local police. PNC was unable to contact WOMBLE regarding the transactions into his PNC account, and the account was closed in February 2021. The remaining balance of $5,397.44 was returned to Victim-5's bank.

32. Based on my training and experience, the PNC 4399 account transactions are not typical of legitimate business activity. Specifically, launderers typically use several methods to rapidly deplete account funds. Methods include purchases of cashier's checks, and multiple transfers through mobile payment services such as Cashapp.

C. Bank Account 3: BB&T

Victim-6

33. Victim-6 is a home builder company located in Charlotte, North Carolina. According to an FBI IC3 report, on February 2, 2021, an employee of Victim-6's company received a fraudulent wire request via email from an individual posing as their company's president. The email was spoofed to appear with the president's email address as the sender. Based on the imposter's instructions, Victim-6's employee initiated a wire transfer of $180,000 to EOE Construction and Sales LLC, BB&T 8217. Bank records show that on February 2, 2021, WOMBLE received the $180,000 wire transfer into his BB&T 8217 from Victim-6. The same day, WOMBLE went to a BB&T Bank branch at 11100 South Lakes Dr., Reston, VA 20191, within the Eastern District of Virginia, and withdrew $6,000 from BB&T 8217.

34. The transaction was identified as fraudulent by Victim-6's employee, and a wire recall was sent from PNC Bank to BB&T on February 18, 2021. A portion of the fraud proceeds, specifically $174,100, was returned to Victim-6.

35. Based on my training and experience, the BB&T 8217 account transactions are not typical of legitimate business activity. Specifically, the fact that the account was opened on

January 22, 2021 and only received the single $180,000 transaction that was later reported as fraudulent, from which funds were immediately withdrawn, before the account's closure on February 22, 2021 suggests fraudulent activity.

D. Bank Account 4: Citibank

Victim-7

36. Victim-7 is a general property management company located in New York. According to an interview with an attorney and an administrator for Victim-7's law firm, they received a settlement of $200,000 on behalf of Victim-7. An employee of the law firm received a request to wire the $200,000 to Victim-7. The transaction did not process because the account number was incorrect.

37. Victim-7's attorney and his administrator stated that on April 14, 2021, an employee of Victim-7's law firm received an email from a person whom they believed was the owner of Victim-7's company. In the email, the ostensible owner stated that the account number on the wire request was incorrect because it was missing a digit. The imposter instructed the employee to wire the money to a different account at Citibank in the name of EOE Construction. The email was not from the owner of Victim-7.

38. According to Victim-7, on April 15, 2021, their law firm's employee wired the money to Citibank 0831 and received an email from the imposter stating, "thank you, wire received."

39. Bank records show that later that day, WOMBLE withdrew $1,000 from Citibank 0831 out of an ATM at a Citibank location at 11800 Spectrum Center Drive, Reston VA, within the Eastern District of Virginia. Between April 16, 2021, and April 20, 2021, WOMBLE withdrew an additional $2,200 over four transactions at the same ATM from Citibank 0831.

During the same period and at the same location, WOMBLE withdrew $196,452.50 in cash over six transactions with tellers from Citibank 0831.

40. An interview with the owner of Victim-7 revealed that on April 27, 2021, he contacted his law firm to tell them he had not received the $200,000. The law firm alerted the owner that they had wired the money. The owner looked at the purported email correspondence between him and the law firm and denied having sent the emails. Some of the emails were sent from Victim-7's actual email while others were sent from email accounts that closely resembled Victim-7's email but with small changes or missing letters. The owner had never heard of WOMBLE or EOE Construction.

41. Based on my training and experience, the Citibank 0831 account transactions are not typical of legitimate business activity. Specifically, the account was opened on March 15, 2021, there was only a single $50 legitimate deposit in March before this large fraudulent transaction from which there were then rapid withdraws. Launderers typically use several methods to rapidly deplete account funds. Methods include high dollar amount cash withdrawals, and rapid and successive ATM withdrawals. Cash withdrawals are often used to buy virtual currency.

Victim-8

42. Victim-8 is a real estate development company located in Brooklyn, New York. An interview with the owner of the company revealed that on April 26, 2021, he reported to the FBI that his company had been a victim of a BEC. Victim-8 was in the process of renovating a building with a construction contractor when he asked for wire instructions. The owner received an email with false wire instructions, resulting in a $75,000 wire transfer being sent from Victim-8's bank

account to Citibank 0831 in the name of EOE TP Interiors LLC. The owner of Victim-8 stated it was discovered later that the construction contractor's email was hacked or compromised.

43. Bank records indicate that on April 23, 2021, WOMBLE received the $75,000 wire into his Citibank 0831. On April 26, 2021, WOMBLE withdrew $1,000 from Citibank 0831 out of an ATM at a Citibank location at 11800 Spectrum Center Drive, Reston VA, within the Eastern District of Virginia. On the same day and location, WOMBLE withdrew $63,730 in cash from Citibank 0831.

44. Based on my training and experience, the Citibank 0831 account transactions are not typical of legitimate business activity. Specifically, the account was opened on March 15, 2021, there was only a single $50 legitimate deposit in March before Victim 7's large transaction, and there were then rapid withdraws. Launderers typically use several methods to rapidly deplete account funds. Methods include high dollar amount cash withdrawals, and rapid and successive ATM withdrawals.

Interview of Patrick Womble

45. On April 30, 2021, agents from the FBI interviewed WOMBLE about the suspicious transactions.

46. WOMBLE initially said that the $75,000 he received into his Citibank account from Victim-8 was from an investor for a house he was flipping. WOMBLE later changed his statement, saying that the money he received was not related to his real estate business but had been sent to him by an UNSUB he met through the internet.

47. WOMBLE told the interviewing agents that, in 2020, he was contacted by the UNSUB in a Google Hangouts chat. WOMBLE believed the UNSUB received his contact information from a website he used to solicit real estate investors. UNSUB offered WOMBLE an

opportunity to make money by allowing the UNSUB to move money through WOMBLE's bank account. WOMBLE agreed and provided the UNSUB with his Wells Fargo Bank account information.

48. WOMBLE further said that he started receiving money in October of 2020, but later stated he began receiving money in September of 2020. On multiple occasions, money was transferred into WOMBLE's bank accounts from unknown sources. The UNSUB provided bank account names and numbers to WOMBLE via Google Hangouts chat with instructions to deposit money into each account. WOMBLE obtained cashier's checks, which he deposited into the accounts at UNSUB's direction. WOMBLE did not know the people from whom he received money or the people to whom he sent money. At UNSUB's direction, WOMBLE also sent money via Cashapp to people he did not know. Also at UNSUB's direction, WOMBLE sent money via virtual currency. WOMBLE would withdraw cash from his bank accounts and deposit it into a virtual currency ATM near his home. The UNSUB would direct WOMBLE where to send the virtual currency.

49. At the UNSUB's direction, WOMBLE opened bank accounts at PNC bank, BB&T and Citibank. He then provided the account details to the UNSUB via Google Hangouts chat. Money was deposited into the accounts, which WOMBLE transferred as the UNSUB directed. PNC, BB&T and Citibank eventually closed WOMBLE's accounts.

50. WOMBLE did not know any of the people or businesses who sent money to him, and he did not know the people to whom he sent money.

51. WOMBLE only communicated about the transfers via Google Hangouts chat and never met anyone in person. WOMBLE understood the money he was receiving was likely not from legitimate business, but he accepted it because he needed money. WOMBLE only profited a

few thousand dollars from moving money because the UNSUB told him that he would get paid after he had done his part.

52. WOMBLE admitted to receiving fraudulent money into his Wells Fargo account, PNC Bank account, and Citibank account.

53. On October 31, 2022, FBI agents conducted a follow up interview with WOMBLE in which he signed a statement acknowledging that all of the information discussed in the previous interview was true.

Conclusion

54. Based on the information contained herein, I respectfully submit that there is probable cause to believe WOMBLE from on or about September, 2020, to on or about April 15, 2021, in the Eastern District of Virginia, and elsewhere, knowingly transferred the proceeds of an unlawful activity with the intent to promote such unlawful activity in order to conceal the proceeds of the unlawful activity in violations of Title 18 United States Code, Section 1956(a)(1)(B) (laundering of monetary instruments).

Respectfully submitted,

Corey Carnahan
Special Agent, FBI
WFO

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on December 13, 2022.

Digitally signed by Ivan Davis
Date: 2022.12.13 14:41:15 -05'00'

The Honorable Ivan D. Davis
United States Magistrate Judge

Alexandria, Virginia